Code-Based Cryptography: New Security Solutions Against a Quantum Adversary

Nicolas Sendrier, Jean-Pierre Tillich

Code-Based Cryptography: New Security Solutions Against a Quantum Adversary

Nicolas Sendrier and Jean-Pierre Tillich

(Teaser:) Cryptography is one of the key tools for providing security in our quickly evolving technological society. An adversary with the ability to use a quantum computer would defeat most of the cryptographic solutions that are deployed today to secure our communications. We do not know when quantum computing will become available, but nevertheless, the cryptographic research community must get ready for it *now*. Code-based cryptography is among the few cryptographic techniques which are known to resist to a quantum adversary.

It has turned out that since their appearance in the mid seventies, public key (or asymmetric) cryptographic primitives have been notoriously difficult to devise and only a handful of schemes have emerged and have survived cryptanalytic attacks. In particular, the security of nearly all public key schemes used today relies on the presumed difficulty of two problems, namely factoring of large integers or computing the discrete logarithm over various groups.

The security of all these schemes was questioned in 1994 when Shor showed that a quantum computer could solve efficiently these two problems [1]. We do not know when large enough quantum computers will be built, but this will have dramatic consequences because it will break all popular public-key cryptosystems that are used in practice today.

It has become clear now that the cryptographic research community has to get ready and has to prepare alternatives. Those alternatives have to be ready, not only for tomorrow in case of a scientific advance (which might even be of a different nature than those that are foreseen today), but also for now, in order to provide long term security (*i.e.* several decades) to the data that is encrypted or digitally signed today. This effort has started already with PQCRYPTO project[1] of the European Horizon 2020 program. Besides, in August, 2015, NSA announced that it is planning to transition "in the not too distant future" to a new cipher suite that is resistant to quantum attacks. The NIST has also released a report on post-quantum cryptography[2] explaining that "we must begin now to prepare our information security systems to be able to resist quantum computing". During the Seventh International Conference on Post-Quantum Cryptography, held in Fukuoka, Japan, in February 2016, NIST has announced that a call for establishing new public key standards that are quantum resistant will be issued by fall 2016.

Code based public key cryptography. Code-based cryptography is one of the main post-quantum techniques available today, together with lattice-based cryptography, multivariate cryptography, and hash-based cryptography. The first code-based cryptosystem was proposed by Robert

[1] `http://cordis.europa.eu/project/rcn/194347_en.html`

[2] `http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf`

McEliece in 1978. It belongs to a very narrow class of public-key primitives that have resisted all cryptanalytic attempts up to now. McEliece's idea was to use as cryptogram a word of a linear error correcting code (a Goppa code in this case) to which random errors were added. The legitimate user, who knows a fast decoding algorithm, can remove the error. The adversary is reduced to a generic decoding problem, which is believed to be hard on average including against a quantum adversary.

France is leader in code-based cryptography and a working group was formed at the end of 2014 to gather French groups working on this topic. It includes in particular two Inria project-teams (one in Paris, one in Saclay), the universities of Limoges and Rouen, and Telecom SudParis. Among the projected actions of this working group, one is to devise a strategy to incite and support initiatives to answer to the forthcoming NIST call, in particular by identifying topics and primitives of interest.

Code-based systems are inherently fast but suffer from a rather large public key size. There have been several recent breakthroughs which reduce the key size to a few thousand bits.

- For instance, systems based on MDPC codes [2] enjoy a strong and novel security reduction and require only very low computing resources, which make them very attractive even for embedded devices.
- Rank metric (instead of the usual Hamming metric) codes provide new code-based primitives [3] with very short keys, relying on similarly hard computational problems, also seem very promising.

Those, together with other more traditional code-based cryptographic solutions, could certainly be part of the new asymmetric cryptographic standards that will emerge in the coming decade.

References

[1] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In FOCS 94, IEEE.

[2] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In ISIT 2013, IEEE.

[3] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. New results for rank-based cryptography. In AFRICACRYPT 2014, Springer.